South Bohemia Mathematical Letters
Volume 29, (2021), No. 1, 41–46.

EULEROVA FAKTORIZAČNÍ METODA

JAROSLAV HORA

ABSTRAKT. Existuje řada metod, jak rozložit složené přirozené číslo N v součin faktorů. Jedním z elementárních postupů je metoda Fermatova, která využívá zápisu čísla N ve tvaru rozdílu čtverců, který je ovšem nutno nalézt: $N = x^2 - y^2$. Půvabná a žákům posledních ročníků ZŠ i středoškolským studentům dostupná je Eulerova metoda. Je využitelná v případě, že N lze zapsat dvěma různými způsoby ve tvaru součtu dvou čtverců přirozených čísel. Takováto vyjádření dnes můžeme nacházet i s pomocí počítače.

ÚVOD

V rámci školské matematiky se žáci seznamují s tématikou rozkladu přirozených čísel v součin prvočísel. V době, kdy teorie čísel vznikala, nalezli metody pro rozklad přirozených čísel v součin faktorů P. Fermat i L. Euler. Jejich metody by byly využitelné i v rámci školské matematiky při práci s talentovanými žáky či studenty středních škol.

1. NÁZEV PRVNÍHO ODDÍLU ČLÁNKU

Pomineme-li metodu opakovaného dělení, je Fermatova faktorizační metoda nejstarší systematickou metodou pro faktorizaci přirozených čísel. Uvidíme, že obecně není příliš efektivní. Je však elementární a občas se vyskytuje ve školských úlohách či v různých matematických soutěžích.

Fermatovou ideou bylo, pokusit se zapsat liché složené číslo N ve tvaru rozdílu čtverců dvou přirozených čísel. Podaří-li se to, pak $N = x^2 - y^2 = (x - y)(x + y)$ a nalezli jsme faktory, na něž se rozkládá číslo N.

Jeden z největších současných badatelů v oblasti faktorizace přirozených čísel, Carl Pomerance, vzpomíná: *„Účastnil jsem se matematické soutěže a jedna z úloh byla rozložit během pěti minut číslo 8 051. Nebylo nám zakázáno používat kapesní kalkulačky, ty tenkrát, okolo roku 1960, kdy se to stalo, vůbec neexistovaly! Nu, v aritmetice jsem byl docela dobrý a věděl jsem, že v časovém limitu mohu zkoušet dělit čísly až do odmocniny z 8 051 (což je zhruba 90). Ale během každého testu, zejména soutěžního, se mnoho studentů pokouší vcítit do mysli osoby, která ho připravila. Jistě by nám nezadali problém, jehož jediný rozumný způsob řešení by spočíval v horečném zkoušení možných dělitelů. Tak jsem strávil několik minut jejím hledáním, zatímco ve mně vzrůstalo znepokojení, že ztrácím příliš mnoho času. Pak jsem opožděně začal s pokusným dělením, jenže čas jsem už skutečně promarnil a úlohu jsem nevyřešil“*. (citováno podle [1]).

Povšimneme-li si, že 8 051 = 8 100 – 49, je řešení snadné a vyžaduje jen znalost vzorce pro rozdíl dvou čtverců: $8\,051 = 90^2 - 7^2 = 97 \cdot 83$. Jak aplikovat Fermatovu metodu v obecném případě, kdy je dáno přirozené číslo N, které se snažíme zapsat ve tvaru $N = x^2 - y^2;\ x, y \in N$?

Received by the editors: 28.02.2022.
2020 Mathematics Subject Classification: 11A51, 101A50.
Key words and phrases: Composite natural numbers, factorization, algorithms for factorization of natural numbers.

Zřejmě musí být $x > \sqrt{N}$, takže vypočteme $m = \lfloor \sqrt{N} \rfloor + 1$, což je nejmenší možná hodnota pro *x* (až na ten případ, kdy *N* je druhou mocninou, $N = x^2$, kdy je vlastně nalezena reprezentace $N = x^2 - 0^2$). Nyní budeme zkoumat, zda číslo $z = m^2 - N$ je čtverec. Pokud ano, nalezli jsme rozklad $N = x^2 - y^2$ a jsme hotovi. Není-li tomu tak, přejděme na další možné *x*, tj. na hodnotu $m + 1$, a vypočtěme $(m + 1)^2 - N = z + 2m + 1$. Opět otestujeme, zda toto číslo je čtvercem atd. Postup i to, jak si zorganizovat zápis výpočtů, bude jasné z následujícího příkladu.

Příklad 1: Rozložme číslo *N* = 3 503 v součin prvočísel s využitím Fermatovy faktorizační metody.

Řešení: Je $\sqrt{N} = 59{,}186\ldots$, číslo *N* není druhou mocninou přirozeného čísla. Máme $m = \lfloor \sqrt{N} \rfloor + 1 = 60$ a číslo $z = m^2 - N = 97$ není čtvercem. Je tedy zapotřebí přejít na číslo *m* + 1 a postup opakovat. Výsledky zapisujeme do Tab. 1.

m	**2 *m* + 1**	***z***
60	121	97
61	123	218
62	125	341
63	127	466
64	129	593
65	131	722
66	133	853
67	135	986
68	137	1121
69	139	1258
70	141	1397
71	143	1538
72	145	$1681 = 41^2$

TABULKA1.

Proč obsahuje tato tabulka ještě prostřední sloupec nadepsaný $2m + 1$? Jak vyplývá z úvah provedených před tímto příkladem, získá se „následující“ hodnota *z* sečtením „původního“ *z* a čísla $2m + 1$. Číslo $z = 218$ ve druhém řádku Tab. 1 se tedy získá tak, že se vrátíme o řádek výše a sečteme $z + (2m + 1) = 121 + 97 = 218$. Obdobně postupujeme i v dalších řádcích až do té doby, kdy zjistíme, že číslo *z* je druhou mocninou. Pak máme $z = 1681 = 41^2 = m^2 - N = 72^2 - 3\,503$, $3\,503 = 72^2 - 41^2 = 31 \cdot 113$.

Příklad 2: Nalezněme rozklad čísla *N* = 10 961.

Řešení: Víme, že musí být $x > \sqrt{N}$, můžeme tedy vypočítat $\sqrt{N} = 104{,}694\ldots$. Vidíme, že *N* není druhou mocninou přirozeného čísla a vypočteme $m = \lfloor \sqrt{N} \rfloor + 1 = 105$, což je nejmenší možná hodnota pro *x*. Nyní budeme zkoumat, zda číslo $z = m^2 - N$ je čtverec: $z = 105^2 - 10\,961 = 64$, platí tedy $10\,961 = 105^2 - 8^2 = 97 \cdot 113$. Ani nemusíme psát tabulku s pomocnými výpočty, výsledek jsme získali hned v prvním kroku.

Příklad 3: Nalezněme rozklad čísla N = 313 591.

Řešení: Víme, že musí být $x > \sqrt{N}$, můžeme tedy vypočítat $\sqrt{N} = 559{,}991 \ldots$. Zjišťujeme, že N není druhou mocninou přirozeného čísla a vypočteme $m = \left[\sqrt{N}\right] + 1 = 560$, což je nejmenší možná hodnota pro x. Nyní budeme zkoumat, zda číslo $z = m^2 - N$ je čtverec: $z = 560^2 - 313\,591 = 9$ a tudíž $313\,591 = 560^2 - 3^2 = 557 \cdot 563$.

Z posledních dvou příkladů vidíme, že Fermatova faktorizační metoda je „rychlá“, pokud se číslo N dá rozložit na dva téměř sobě rovné faktory. Chápeme teď, proč se v RSA šifrovací metodě doporučuje volit prvočísla p, q mající „různou bitovou délku“, různý počet cifer.

Naopak by nebylo moudré vzít za p, q kupř. dvě „po sobě jdoucí“ prvočísla. Následující příklad ukáže bohužel daleko typičtější situaci.

Příklad 4: Nalezněme rozklad čísla N = 10 237.

Řešení: Je $\sqrt{N} = 101{,}178$ ... a máme tuto tabulku:

m	$2m+1$	z		m	$2m+1$	z
102	205	167		147	295	11 372
103	207	372		148	297	11 667
104	209	579		149	299	11 964
105	211	788		150	301	12 263
106	213	999		151	303	12 564
107	215	1212		152	305	12 867
108	217	1427		153	307	13 172
109	219	1644		154	309	13 479
110	221	1863		155	311	13 788
111	223	2084		156	313	14 099
112	225	2307		157	315	14 412
113	227	2532		158	317	14 727
114	229	2759		159	319	15 044
115	231	2988		160	321	15 363
116	233	3219		161	323	15 684
117	235	3452		162	325	16 007
118	237	3687		163	327	16 332
119	239	3924		164	329	16 659
120	241	4163		165	331	16 988
121	243	4404		166	333	17 319
122	245	4647		167	335	17 652
123	247	4892		168	337	17 987

124	249	5139		169	339	18 324
125	251	5388		170	341	18 663
126	253	5639		171	343	19 004
127	255	5892		172	345	19 347
128	257	6147		173	347	19 692
129	259	6404		174	349	20 039
130	261	6663		175	351	20 388
131	263	6924		176	353	20 739
132	265	7187		177	355	21 092
133	267	7452		178	357	21 447
134	269	7719		179	359	21 804
135	271	7988		180	361	22 163
136	273	8259		181	363	22 524
137	275	8532		182	365	22 887
138	277	8807		183	367	23 252
139	279	9084		184	369	23 619
140	281	9363		185	371	23 988
141	283	9644		186	373	24 359
142	285	9927		187	375	24 732
143	287	10 212		188	377	25 107
144	289	10 499		189	379	25 488
145	291	10 788		190	381	25 863
146	293	11 079		191	383	26 244

TABULKA 2.

26 244 = 162^2. Konečně! Nyní máme $z = 162^2 = m^2 - N = 191^2 - 10\,237,\ 10\,237 = 29 \cdot 353$.

Takto tedy vypadá „nepřikrášlený“ průběh Fermatovy metody. (Ve školní třídě by bylo možné práci rozdělit: je třeba pro každé m = 102, 103, ... vypočítat číslo $z = m^2 - 10\,237$ a zjistit, zda je či není druhou mocninou – na každého žáka by tak vyšlo ověření 3 – 4 řádků tabulky).

Teď je na místě otázka, zda Fermatova faktorizační metoda obecně skončí v konečném počtu kroků. Je tomu tak, neboť každé liché složené číslo $a \cdot b$ lze zapsat jako rozdíl dvou čtverců: $a \cdot b = \left(\frac{1}{2}(a+b)\right)^2 - \left(\frac{1}{2}(a-b)\right)^2$.

Jak již víme, Fermatova metoda umožňuje rychle rozložit číslo *N*, které má dva faktory téměř sobě rovné, tedy blízké $\sqrt{N}$. To je bohužel dost nepravděpodobný případ. V knize [1] se kupř.

ukazuje, že je-li *N* součinem dvou faktorů *a, b; a* ≈ $N^{\frac{1}{3}}$, $b \approx N^{\frac{2}{3}}$, pak lze počet kroků potřebných k proběhnutí algoritmu odhadnout jako $\frac{1}{2} N^{\frac{2}{3}}$.

Fermatova metoda je horší než metoda opakovaného dělení, a tudíž je pro faktorizaci velkých čísel prakticky nepoužitelná. Je to však metoda jednoduchá a snad by informace o ní mohla být využitelná ve škole, resp. v matematickém kroužku.

2. EULEROVA FAKTORIZAČNÍ METODA

Fermatova metoda je horší než metoda opakovaného dělení a tudíž je pro faktorizaci velkých čísel prakticky nepoužitelná. Je to však metoda jednoduchá a snad by informace o ní mohla být využitelná ve škole, resp. v matematickém kroužku.

Co když lze přirozené číslo *N* zapsat jako součet dvou čtverců: $N = a^2 + b^2; a, b \in N$? To ještě zřejmě není dostatečná informace, která by pomohla nalézt rozklad čísla *N*. Někdy se však stane, že existuje dokonce dvojí vyjádření čísla *N* ve tvaru součtu čtverců: $N = a^2 + b^2$, $N = c^2 + d^2$, kdy se dvojice *a*, *b* a *c*, *d* neliší jen pořadím sčítanců. Je např. 221 = 52 + 142 = 102 + 112, 377 = 42 + 192 = 112 + 162, 629 = 22 + 252 = 102 + 232. Euler ukázal, jak lze tuto situaci využít k nalezení rozkladu čísla *N*. Můžeme předpokládat, že číslo *N* je liché, a tedy je tvaru $N = 4k + 1; k \in N$. (Čísla tvaru $N = 4k + 3$ zjevně nelze zapsat ve tvaru $N = a^2 + b^2$).

Jestliže *N* je liché a $N = a^2 + b^2$, pak je jedno z čísel *a*, *b* liché a druhé sudé: nechť tedy *a* je liché. Je-li dále $N = c^2 + d^2$, pak opět předpokládejme, že *c* je liché a od rovnosti $a^2 + b^2 = c^2 + d^2$ přejděme k $a^2 - c^2 = d^2 - b^2$. Je tedy

$$(a - c)(a + c) = (d - b)(d + b). \tag{1}$$

Spočtěme největší společný dělitel rozdílů $D(a - c, d - b) = k$. Tento výsledek jsme zvýraznili tučně, je podstatný a budeme jej spolu s třemi dalšími potřebovat při ověření výpočtu. Povšimněme si, že *k* je sudé číslo. Vydělením pak máme

$$a - c = k \cdot l, d - b = k \cdot m, D(l, m) = 1. \tag{2}$$

Získali jsme tři ze čtyř potřebných čísel k určení rozkladu *N*. Dosaďme ze (2) do (1) a zkraťme *k*:

$$l \cdot (a + c) = m \cdot (d + b). \tag{3}$$

Vzhledem k nesoudělnosti čísel *l* a *m* dělí *m* součet $a + c$, tj.

$$a + c = m \cdot n. \tag{4}$$

Nalezli jsme čtvrté hledané číslo a dosadíme-li za *a* + *c* do (3) a zkrátíme *m*, je

$$d + b = l \cdot n. \tag{5}$$

Ze (4) a (5) plyne, že $n = D(a + c, d + b)$. A protože *a* + *c* i *d* + *b* jsou sudá čísla, je i *n* sudé. Teď již můžeme napsat, jak vypadá rozklad čísla *N* v součin:

$$N = \left(\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2\right) \cdot (m^2 + l^2).$$

Ověřme tuto rovnost. Roznásobením pravé strany máme

$$\frac{1}{4}\left(\left(k^2 + n^2\right)\left(m^2 + l^2\right)\right) = \frac{1}{4}\left(\left(km\right)^2 + \left(kl\right)^2 + \left(nm\right)^2 + \left(nl\right)^2\right).$$

Dosadíme-li sem ze (2), (4) a (5), obdržíme

$$\frac{1}{4}((km)^2+(kl)^2+(nm)^2+(nl)^2)=\frac{1}{4}((d-b)^2+(a-c)^2+(a+c)^2+(d+b)^2)$$
$$=\frac{1}{4}(2a^2+2b^2+2c^2+2d^2)=\frac{1}{4}(2N+2N)=N.$$

Vzorec platí a poskytuje rozklad čísla *N*.

Příklad 5: Jak jsme uvedli, je $377=4^2+19^2=11^2+16^2$. Pišme tedy $19^2-11^2=16^2-4^2$. Rozdíl čtverců s lichými základy $a^2-c^2=19^2-11^2$ poskytuje $a-c=8, a+c=30$, podobně $d-b=12, d+b=20$. Dále $D(a-c,d-b)=k=4$, dále máme $l=2$, $m=5$ a nakonec $n=6$. Pak již snadno objevíme rozklad $377=13\cdot 29$. V daném případě jde dokonce o rozklad prvočíselný, jindy bychom museli při hledání úplného prvočíselného rozkladu ještě faktorizovat jednotlivé činitele, což bývá úloha výrazně snazší než úloha prvotní.

Příklad 6: Euler se proslavil rozkladem čísla $N = 1\,000\,009$, které bylo mylně považováno za prvočíslo. Je $N = 1000^2 + 3^2$. Euler nalezl další rozklad $N = 235^2 + 972^2$. Ne, žádné prvočíslo, jde o složené číslo! Aplikací jeho metody máme $235^2 - 3^2 = 1000^2 - 972^2$, $a-c=232$, $a+c=238$, podobně $d-b=28$, $d+b=1972$. Spočteme $D(232,28)=4=k$ a dale $l=\frac{232}{4}=58$, $m=\frac{28}{4}=7$, $n=\frac{238}{7}=34$. Dosazením do výše uvedeného vzorce nacházíme rozklad $1\,000\,009=293\cdot 3\,413$.

V dnešní počítačové době můžeme v programu Mathematica experimentovat s nacházením řešení diofantické rovnice $x^2+y^2=N$ asi takto:

```
Reduce[x^2+y^2==1000009&&x>0&&y>0,{x,y},Integers]
(x==3&&y==1000)||(x==235&&y==972)||(x==972&&y==235)||(x==1000&&y==3)
Reduce[x^2+y^2==6001&&x>0&&y>0,{x,y},Integers]
(x==15&&y==76)||(x==49&&y==60)||(x==60&&y==49)||(x==76&&y==15)
Reduce[x^2+y^2==629&&x>0&&y>0,{x,y},Integers]
(x==2&&y==25)||(x==10&&y==23)||(x==23&&y==10)||(x==25&&y==2)
```

Hlavní nevýhodou Eulerovy faktorizační metody je ovšem to, že není univerzální, ale je možné ji užít jen k faktorizaci speciální podmnožiny množiny přirozených čísel. I faktory získané jejím užitím mají tvar $4k+1$, $k \in \mathbb{N}$. Je to však metoda pozoruhodná a mohla by sloužit k procvičení znalostí probíraných již na základní škole (výpočet největšího společného dělitele, schopnost dosazení do vzorce atd.).

Poznamenejme ještě, že P. Fermat přišel s domněnkou, že každé prvočíslo tvaru $4k+1$ lze jednoznačně zapsat jako součet dvou čtverců přirozených čísel. S existenčním důkazem tohoto tvrzení přišel r. 1749 L. Euler a s nalezením přirozených čísel a, b do součtu $p = a^2 + b^2$ roku 1801 K. F. Gauss. H. J. S. Smith nalezl elementárnější metodu pro určení čísel a, b a v moderní době uvedl Brillhart metodu umožňující velice rychlý počítačový výpočet čísel a, b i pro obrovská prvočísla tvaru $4k+1$.

LITERATURA

[1] von zur Gathen, J., Gerhard, J.: *Modern Computer Algebra*, Cambridge Univ. Press, 1999, ISBN 0 521 64176 4.

[2] Ore, O.: *Number Theory and Its History*, Dover Publications, 1988, ISBN 0 048 665620 9.

[3] Riesel, H.: Prime Numbers and Computer method for Factorization, Springer, 2012, ISBN 978-0-8176-8298-9.

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY FPE ZČU PLZEŇ, ČESKÁ REPUBLIKA
E-mail address: horajar@kmt.zcu.cz